UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,667	02/05/2004	Mukesh Kumar Singh	TI-35979	5588

23494 7590 01/23/2009

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
01/23/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/772,667	SINGH, MUKESH KUMAR	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are pending in this application.

2. Claims 3-4 are currently amended.

Claim Objections

3. Claims 1 and 13 are objected because of the following:

As to claim 1, input message is partitioned into matrix element in step (a) and a determinant of said matrix is computed in step (b). Although determinants can be computed only from square matrices, Applicant didn't mention in any of the claimed steps that the matrix had to be square matrix. It should be noted that it's not possible to find a determinant of an non-square matrix; thus claimed matrix couldn't be just any type of matrix.

As to claim 13, a determinant is computed from a matrix-based encrypted message matrix is step (a); thus, it is objected for the same reason as claim 1.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1 and 13 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: 1) a preprocessing random permutation of the data (message) and 2) when determinant of matrix is 0 or 1, then exit the procedure by returning "encryption failed" and try

the encryption again with a new set of fields (e.g., a new time stamp in the message) (see Specification, page 8). It should be noted that Applicant admitted that: "no data block on the principal diagonal is allowed to be zero" and Applicant further clarified that "if the block size used is on the order of 64 bytes, then this condition will essentially never arise after a preprocessing random permutation of the data (message) (see Specification, page 8). Although Applicant mentioned that probability of computing the determinant to be zero or one is only 2/n where n is the public key modulus; Applicant didn't provide any evidence or explanation that this situation will never occur; thus, step 2 is also essential.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re *Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).*

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that

accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state. Since Applicant's method steps are not tied to a particular machine and do not perform a transformation, the claims are non-statutory.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-8 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandstrom (Patent No.: 4,322,577) and further in view of Chen et al. (Patent No.: US 7,263,191 B2) (hereinafter, "Chen").

10. As to claim 1, Brandstrom discloses A method of encryption, comprising:

(a) partitioning an input message into matrix elements (col. 3, lines 40-45);

(b) computing a determinant of said matrix (col. 6, lines 4-10 and lines 55-63);

Although Brandstrom discloses multiplying said matrix by a determinant (col. 6, lines 40-45 and col. 7, lines 16-30), Brandstrom doesn't explicitly disclose (c) encrypting said determinant.

However, Chen discloses (c) encrypting a determinant (col. 3, lines 30-62, Chen teaches this concept by encrypting each share with an encryption key). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of

Brandstrom as taught by Chen in order to increase the integrity of data which transmitted over public network.

11. As to claim 2, Brandstrom discloses further comprising, preprocessing said input message wherein said preprocessing includes a permutation of the message (col. 7, lines 4-15).

12. As to claim 3, Brandstrom discloses wherein: (a) said permutation of step (a) of claim 2 is generated by a hash of said input message (col. 6, lines 40-45 and col. 7, lines 16-30).

13. As to claim 4, Brandstrom discloses wherein: (a) said permutation of step (a) of claim 2 is generated by a random sequence (col. 6, lines 55-63).

14. As to claim 5, Brandstrom discloses wherein: (a) said preprocessing of step (a) of claim 2 includes exclusive ORing said message after permutation with generators of said permutation (col. 7, lines 29-65).

15. As to claim 6, Brandstrom discloses wherein: (a) said encrypting of step (c) of claim 1 is public-key encryption (col. 7, lines 29-65).

16. As to claim 7, Brandstrom discloses wherein: (a) said public-key encryption is RSA (col. 7, lines 29-65).

17. As to claim 8, Brandstrom discloses wherein: (a) said partitioning of step (a) of claim 1 first fills the principal diagonal of said matrix (col. 7, lines 29-65).

18. As to claim 13, it is rejected using the same rationale as for the rejection of claim 1.

19. As to claim 14, it is rejected using the same rationale as for the rejection of claim 2.

20. Claims 9-12 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boylan et al. (Pub. No.: US 2003/0028484 A1) (hereinafter "Boylan") and further in view of Brandstrom.

21. As to claim 9, Boylan discloses a method of encryption, comprising:

(a) defining a permutation source ([0008], lines 14-15);

(b) generating a permuted message for an input message employing said permutation source ([0008], lines 14-15);

(c) padding said permuted message with said permutation source to obtain a preprocessed message ([0008], lines 16-18).

Although Boylan discloses encrypting said preprocessed message ([0008], lines 20-21), Boylan doesn't explicitly disclose (d) encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message.

However, Brandstrom discloses (d) encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message (col. 2, lines 50-65,

Brandstrom provides DES as block-based encryption which divides long message into smaller blocks and encrypts the individual blocks).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Boylan as taught by Brandstrom in order to encrypt long messages by taking advantage of standard block-based encryption method.

22. As to claim 10, Boylan discloses wherein: said permutation source is generated by a hash of said input message ([0008], lines 14-15).

23. As to claim 11, Boylan discloses wherein: said permutation source is generated by a random sequence ([0008], lines 14-15).

24. As to claim 12, Boylan discloses wherein: said block-based encryption is a public key encryption ([0008]).

25. As to claim 15, Boylan discloses wherein said padding includes prepending said permuted message with said permutation source to obtain said preprocessed message ([0008], lines 14-15).

26. As to claim 16, Boylan discloses wherein said padding includes appending said permuted message with said permutation source to obtain said preprocessed message ([0008]).

27. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the Applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

28. Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435